All Features in TCU02/SIU02 SW T14B

Feature Description

The latest versions of feature descriptions are found in Feature Store

221 04-FGB 101 645 Rev G

Contents

1 Content Summary

Available Features in current and the previous three Releases.

1/O = Version 1 / Optional Feature
2/B = Version 2 / Basic Feature

Feature number	Feature name	T12B	T13B	T14A	T14B
FAJ 121 2547	1588v2 Transparent Clock	1/O	1/O	1/O	1/O
FAJ 121 2546	Auto Integration without laptop (SON)	1/B	1/B	1/B	1/B
FAJ 121 0907	Bidirectional Forwarding Detection	1/O	1/O	1/O	1/O
FAJ 121 4039	Centralized User Management				1/O
FAJ 121 4042	Certificate FQDN Lookup				1/B
FAJ 121 0679	Circuit Emulation	2/O	2/O	2/O	2/O
FAJ 121 2968	DHCP Relay for IPv6 in SIU/TCU		1/B	1/O	1/O
FAJ 121 0727	DHCP Relay in SIU/TCU	1/B	1/B	1/B	1/B
FAJ 121 1852	Ethernet Bridging	1/B	1/B	1/B	1/B
FAJ 121 0909	Ethernet OAM	1/O	1/O	1/O	1/O
FAJ 121 1856	Expanded SFP Support	1/B	1/B	1/B	1/B
FAJ 121 0680	Frequency Synchronization Client with NTP over IP	2/O	2/B	3/B	4/B
FAJ 121 0683	Frequency Synchronization Client with PTP over IP	2/O	2/O	3/O	4/O
FAJ 121 2185	G.826 and TDM loopback	1/B	2/B	2/B	2/B
FAJ 121 1848	IP Loopback	1/B	1/B	1/B	1/B
FAJ 121 0677	IP over E1/T1	3/O	3/O	3/O	3/O
FAJ 121 3783	IPsec client for SIU/TCU			1/O	1/O
FAJ 121 2548	IPv6 Basic Functionality	1/O	2/O	2/O	2/O
FAJ 121 1849	Layer 3 ACL	1/B	1/B	1/B	1/B
FAJ 121 1850	Multiple Uplinks	1/B	1/B	1/B	1/B
FAJ 121 2545	OSPFv2 Dynamic Routing	1/O	1/O	1/O	1/O
FAJ 121 0912	Policy Based Routing (PBR)	1/O	1/O	1/O	1/O
FAJ 121 3782	QoS Remarking and Policing			1/O	1/O
FAJ 121 4038	Real- time Security event logging				1/O
FAJ 121 4041	Remote System Logging				1/B
FAJ 121 0703	Site LAN	1/B	1/B	1/B	1/B
FAJ 121 0756	STN Local Port Security	1/B	1/B	1/B	1/B
FAJ 121 0913	Synchronous Ethernet	1/O	2/O	2/O	2/O
FAJ 121 3781	System Improvements in SIU T14A			1/B	1/B
FAJ 121 4034	System Improvements in SIU T14B				1/B
FAJ 121 0702	Transport Sharing	1/B	1/B	1/B	1/B
FAJ 121 2549	TWAMP Responder	1/O	1/O	1/O	1/O

FAJ 121 0704	VLAN	1/B	1/B	1/B	1/B
FAJ 121 3241	Y.1731 Initiator		1/O	1/O	1/O

2 General - BASIC FEATURES

2.1 Auto Integration without laptop (SON)

Feature Identity:	FAJ 121 2546/1, Rev. B
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

2.1.1 Attention

Commercial attention

NOTE! This feature only enables Auto Integration of the SIU/TCU portion of the radio base station, i.e. RBS 2000, RBS 3000 and RBS 6000. For other components of the radio base station additional liceneses are required. For any given radio standard, please consult auto integration description for that specific RAN.

Dependencies

No internal technical dependencies have been defined for this Feature

2.1.2 Summary

The installation of new RBS equipment at the cell site has traditionally required substantial expertise and effort in terms of management system connection and equipment start-up. In this step towards the Self Organizing Network (SON), the installer, equipped with just the equipment serial number and site ID, can initialize new RBS equipment using only a smart phone.

NOTE! This feature only enables Auto Integration of the SIU/TCU portion of the radio base station, i.e. RBS 2000, RBS 3000 and RBS 6000. For other components of the radio base station additional liceneses are required. For any given radio standard, please consult auto integration description for that specific RAN.

2.1.3 Benefits

By substantially reducing the configuration effort and expertise required for new RBS equipment, the operator is able to start using his new investment more quickly than in the past, without committing highly-qualified personnel to long and costly site visits.

2.1.4 Description

The equipment start-up procedure is initiated by the installer collecting site ID and DU serial numbers. These are sent via smart-phone to the OSS-RC, which links the RBS to the site and commences the start-up process.

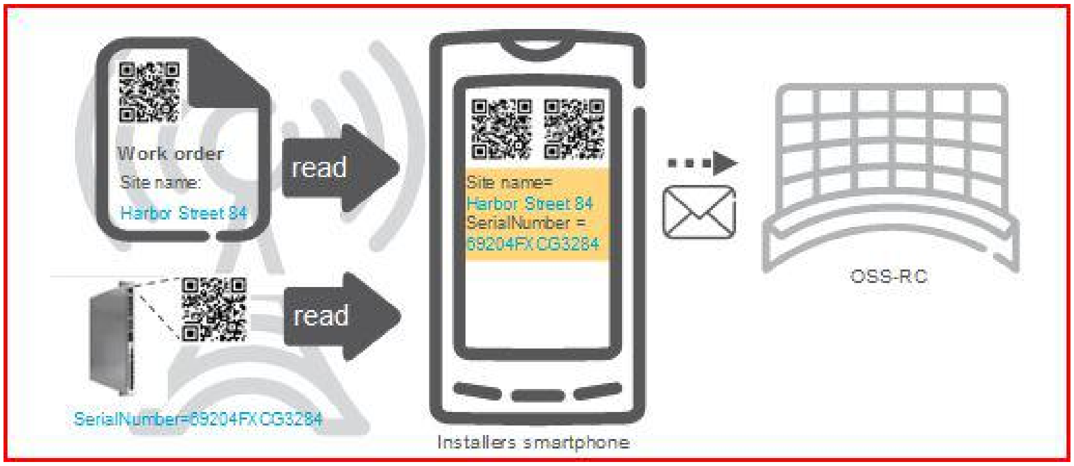


Figure Site ID and DU serial number are retrieved and sent to OSS-RC

The RBS is now powered up.

First, the RBS scans the VLANs to which it is connected. It locates and contacts DHCP to obtain its IP address and addresses to OSS and COMINF servers. It also obtains an NTP synchronization signal to calibrate its internal highly-stable oscillator.

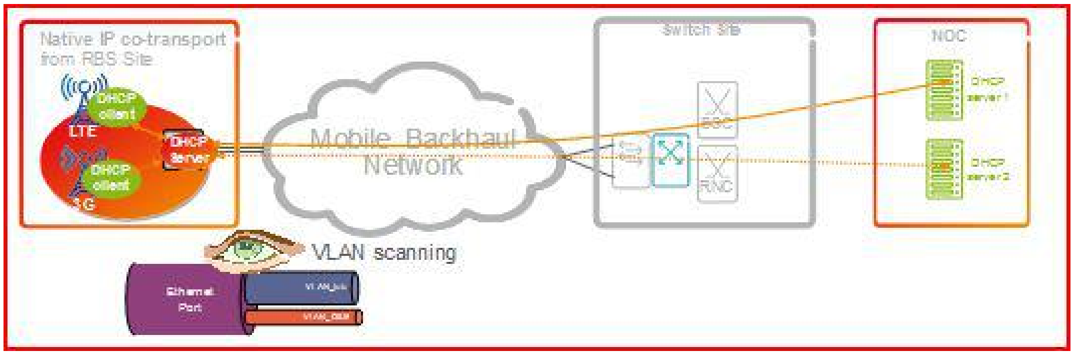


Figure RBS scans VLANs to locate DHCP servers.

The TCU/SIU authenticates itself towards the OAM system using an Ericsson certificate installed during RBS production, and in return automatically receives a signed operator certificate.

These are followed by several more automatic set-up procedures for O&M, traffic interfaces and radio network configuration before OSS finally activates the cells covered by the RBS.

2.2 Certificate FQDN Lookup

Feature Identity:	FAJ 121 4042/1, Rev. A
Feature Type:	Basic in T14B
Technology:	

2.2.1 Attention

Commercial attention

Not applicable

Dependencies

No technical dependencies have been defined for this Feature

2.2.2 Summary

The Certificate FQDN look up feature adds DNS resolver functionality to the SIU so hostnames/FQDNs (Fully Qualified Domain Names) can be used instead of or interchangeably with IPv4 IP-addresses, for a defined set of use cases.

2.2.3 Benefits

The operator can configure search domains for extended lookup using IP addresses and/ or hostnames/FQDNs (Fully Qualified Domain Names), for a defined set of use cases.

2.2.4 Description

The DNS resolver feature enables user for DNS lookup which allows resolving IPv4 address from Fully Qualified Domain Name (FQDN). It means that hostnames can be used interchangeably with IP-addresses, for a defined set of use cases. Up to two IP addresses of DNS servers can be configured.

Example of supported use cases:

- Allows certificates to use FQDN instead of IP addresses

- Certificate Revocation Lists (CRL) Distribution Point can use FQDN instead of IP address.

- Hostname/FQDN support in CLI commands for certificate management.

- Hostname/FQDN support in configuration of Remote Syslog and Centralized User Management (server addresses).

- Hostname/FQDN support in CLI commands that maps directly to underlying Linux commands, e.g. ping, traceroute

2.3 DHCP Relay in SIU/TCU

Feature Identity:	FAJ 121 0727/1, Rev. B
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	

2.3.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.3.2 Summary

The DHCP relay feature enables the SIU/TCU to provide DHCP services to connected IP enabled RBSs and other equipment.

The main use case is to support the auto installation features in WCDMA and LTE RBSs.

The technical implementation of the feature is a BOOTP relay agent as specified in RFC 1542 Section 4.

2.3.3 Benefits

The customer benefit is the ability to provide DHCP services to the RBS site.

The feature is primarily intended to be used with the RBS auto integration features for WCDMA and LTE RBSs, but it can also be used to provide DHCP services to arbitrary equipment at the RBS site.

2.3.4 Description

This feature uses a BOOTP relay agent as specified in RFC 1542 Section 4.

DHCP requests from equipment on the RBS site will be forwarded to a DHCP server, typically in the OSS-RC.

It is possible to implement up to 8 BOOTP relay agents in the SIU/TCU. Any IP-subnet in the SIU/TCU can be attached to one relay agent, except those IP-subnets that are used for uplink. This means that multiple agents can run on different (untagged) Ethernet ports or on the same Ethernet port on different VLANs.

For each instance of the BOOTP relay agent it is possible to individually configure the IP address of the DHCP server to which requests should be forwarded.

2.4 Ethernet Bridging

Feature Identity:	FAJ 121 1852/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

2.4.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.4.2 Summary

The new Ethernet bridging feature enables the TCU/SIU to act as a bridge in addition to existing router functionality. Multiple bridging and routing instances can be configured on a single TCU/SIU.

The use of BVI (Bridged Virtual Interfaces) facilitates efficient use of bridging and routing simultaneously in the same TCU/SIU.

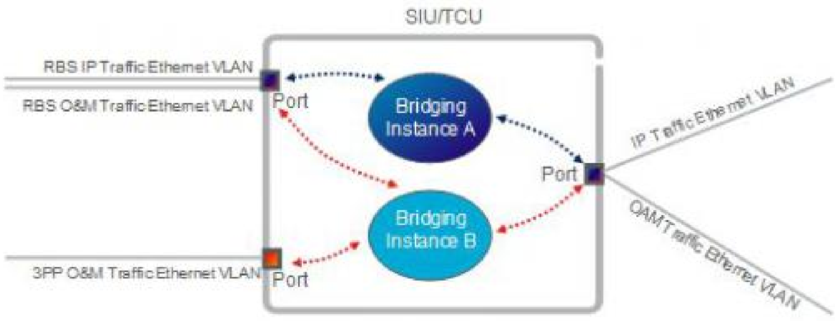
2.4.3 Benefits

The main motivation for this feature is to allow the TCU/SIU to be added easily to legacy 3G IP over Ethernet networks, in which the Node B is connected directly to the Transport network. If the TCU/SIU were only able to act as a router, extensive IP address re-configuration within the network would be required, but the bridging function is transparent to Ethernet provided that VLAN identities on either side of the bridge are the same.

For example, an operator may have existing 3G services based on IP over Ethernet transport (no TCU/SIU required for single RAN). If the operator wishes to add LTE to the site, transport sharing via an TCU/SIU is needed so that both traffic types can share a single uplink. Adding a TCU/SIU with bridging is convenient for the 3G traffic as no address configuration changes are needed. Adding LTE to the site is then an easy new installation.

2.4.4 Description

The bridging function allows the TCU/SIU to forward Ethernet payload without needing to configure the full IP address plan that would be required if the traffic were to be routed. This is of particular value if the TCU/SIU is being introduced to an existing network.


SIU/TCU
RBS IP Traffic Ethernet VLAN
RBS O&M Traffic Ethernet VLAN
Port
Bridging Instance A
Port
IP Traffic Ethernet VLAN
Bridging Instance B
OAM Traffic Ethernet VLAN
3PP O&M Traffic Ethernet VLAN
Port

Both untagged and tagged VLANs are supported; tagged VLANs offer the possibility for multiple VLANs to share the same physical ports and links, and for traffic to be prioritized into eight Classes of Service (CoS) using IEEE802.1p "p-bit" marking.

Several bridging instances can be configured in the TCU/SIU, to accommodate the requirements of IP payload traffic or O&M flows. At the same time multiple routing instances can also be configured; these are required by GSM or CDMA RBSs connected to the TCU/SIU via E1 or T1 links. Abis over IP is not used with the bridging function and must always be routed. Routed and bridged VLANs can share common physical ports and transport network links, taking full advantage of the aggregation benefits of co-transport for GSM, WCDMA, CDMA and LTE services.

2.4.4.1 Standards

IEEE 802.1D

2.5 Expanded SFP Support

Feature Identity:	FAJ 121 1856/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

2.5.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.5.2 Summary

Fast Ethernet SFPs can now be used at the TCU/SIU Ethernet ports in addition to the previously supported GE modules.

2.5.3 Benefits

Support for additional types of SFP adds flexibility for the operator to use different types of connectivity for both transport and Site LAN equipment.

2.5.4 Description

Support for the following Fast Ethernet SFPs is added in TCU/SIU T11A:

- SFP 100Base-LX10 (SM, 1310nm, 13dB, 10km)
- SFP 100Base-FX (MM, 1310nm, 13dB, 2km)

Support for the following Gigabit Ethernet SFPs continues:

- SFP Module 1000Base-SX (850nm, MM LC-connector)
- SFP Module 1000Base-LX (1310nm, MM/SM, LC-connector)

- SFP Module 1000Base-LX
- SFP Module 1000Base ZX (1550nm, SM, LC-connector)

2.6 Frequency Synchronization Client with NTP over IP

Feature Identity:	FAJ 121 0680/4, Rev. A
Feature Type:	Basic in T14B
Technology:	GSM, WCDMA, LTE

2.6.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.6.2 Summary

This feature enables NTP frequency synchronization for an IP-only connected SIU/TCU. It provides the Sync Client part in SIU/TCU. This feature calibrates the SIU/TCU clock so that a connected RBS can generate radio frequency according to the 3GPP specification.

2.6.3 Benefits

This feature enables frequency synchronization of the RBS via the SIU/TCU using standard NTP protocol over the IP backhaul. This solution is cost efficient compared to the alternative of providing an external clock source, such as a GPS receiver.

The feature also supports quick roll-out of new IP-based RBSs, or move from TDM to IP backhaul, as no synchronization support in the transport network is required.

2.6.4 Description

Frequency synchronization for an SIU/TCU is achieved by aligning the frequency of the SIU/TCU to the frequency of an NTP-based Sync Server with traceability to a G.811 source.

The SIU/TCU's Sync Client sets up an association with the sync server. The Sync Client will request time stamps from the Sync Server. An Ericsson patented algorithm in the Sync Client filters the time stamps and calculates the frequency drift of the RBS clock. The clock is regulated to give < 50ppb radio transmission frequency deviation.

The long term stability clock is calibrated at the time of production. The frequency stays within range for up to 6 months when the unit is without power or without a calibration source. When the SIU/TCU is put into operation the NTP packets and the filter algorithm determine if the clock is drifting, and adjustments are made if needed.

The synchronization reference of the synch server is required to have a long term frequency accuracy of better than 10E-11, i.e. traceable to a PRC or GPS. There are no specific requirements on the sync server for Packet delay or Packet Delay Variation.

The Packet Delay (PD) and packet delay variation (PDV) in the access network between the NTP server and the NTP client in the SIU/TCU is in practice less important because of the long filtering time used for frequency synchronization, provided the SIU/TCU has been synchronized within the last 4 months and any high PDV situation does not persist longterm. A faster algorithm is used for initial calibration. This faster algorithm is used for initial calibration when the backhaul network is good enough (low enough packet delay variation). If the PDV is too large for the fast algorithm, the calibration will fall back to using the slow algorithm.

2.6.5 Enhancement

The enhancement enables the faster algorithm for initial calibration also after sync server re-selection (only applicable when calibrating the first time after restart). This reselection could for instance take place if the synchronization server with highest priority is not available at startup of the SIU/TCU.

2.7 G.826 and TDM loopback

Feature Identity:	FAJ 121 2185/2, Rev. B
Feature Type:	Basic in T13B, T14A, T14B
Technology:	

2.7.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.7.2 Summary

The SIU/TCU now gathers PM data from E1/T1 interfaces according to G.826. The SIU/TCU, if so configured, responds to remote loopback commands. A CLI-command is available for timed loopback of selected interfaces.

2.7.3 Benefits

Standardized PM reporting for TDM intefaces enables verification of service level agreements and aids in trouble shooting.

The loopback function enables efficient validation of TDM services, at installation or for trouble shooting

2.7.4 Description

The PM counters for G.826 are enabled and reported as all other PM counters in the SIU/TCU.

Remote loopback for TDM interfaces is enabled by an attribute on the E1/T1 managed object.

A CLI-command is available for timed loopback of selected interfaces.

2.7.4.1 Standards

G.826, G.704

2.7.5 Enhancement

The /2 revision of the feature adds the possibility to use timed loopback, i.e. an interface can be set in loopback for a specified time and then automatically reverts back to it's previous state.

2.8 IP Loopback

Feature Identity:	FAJ 121 1848/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

2.8.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.8.2 Summary

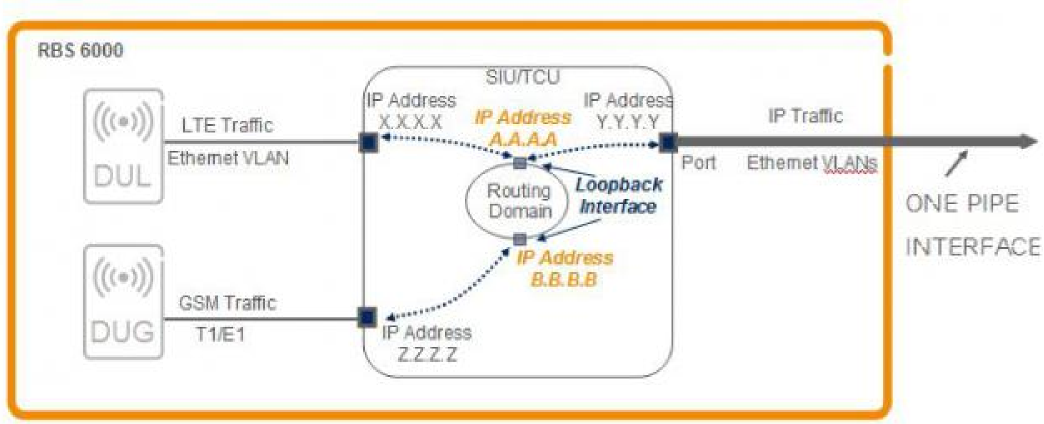
IP services at the TCU/SIU depend on an IP interface to terminate traffic. In the past, an IP interface has been bound only to a physical network interface. The IP loopback interface provides an IP termination point that is not associated with a particular physical interface. Traffic to/from the loopback interface can be routed via alternate physical interfaces.

2.8.3 Benefits

In the past, only one uplink port (either IP/Ethernet or IP over E1/T1) was available for WAN at the TCU/SIU. In T11A the concept of multiple uplink ports is introduced.

When only one port is used for uplink, the port's own IP address is used to identify the TCU/SIU at the switch site. When more than one port is used for uplink, each one has a separate IP address. It would be possible for the TCU/SIU to be identified using the addresses of each of its WAN interfaces, but this is impractical when multiple paths exist between the same two nodes.

2.8.4 Description



To simplify addressing issues a single virtual interface (loopback interface) is configured on the TCU/SIU. The IP address assigned to this interface (loopback address) is used as a common source address for all IP traffic being sent from the TCU/SIU. This is particularly useful for management purposes, as it prevents packets being allocated different source addresses according to the port used.

The loopback interface is permanent, in that it will remain in use until explicitly removed from the configuration. In this way, the switch site node sees a single IP address (the loopback address) at the TCU/SIU and will select a transmission path to that address from those available. The removal of a particular path due to a fault will not affect the reachability of the remote site, provided of course that at least one link remains active.

Usually one loopback address will be assigned at each TCU/SIU; there are, however, circumstances where more than one virtual interface is required and this can be configured.

2.9 Layer 3 ACL

Feature Identity:	FAJ 121 1849/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	

2.9.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.9.2 Summary

Summary

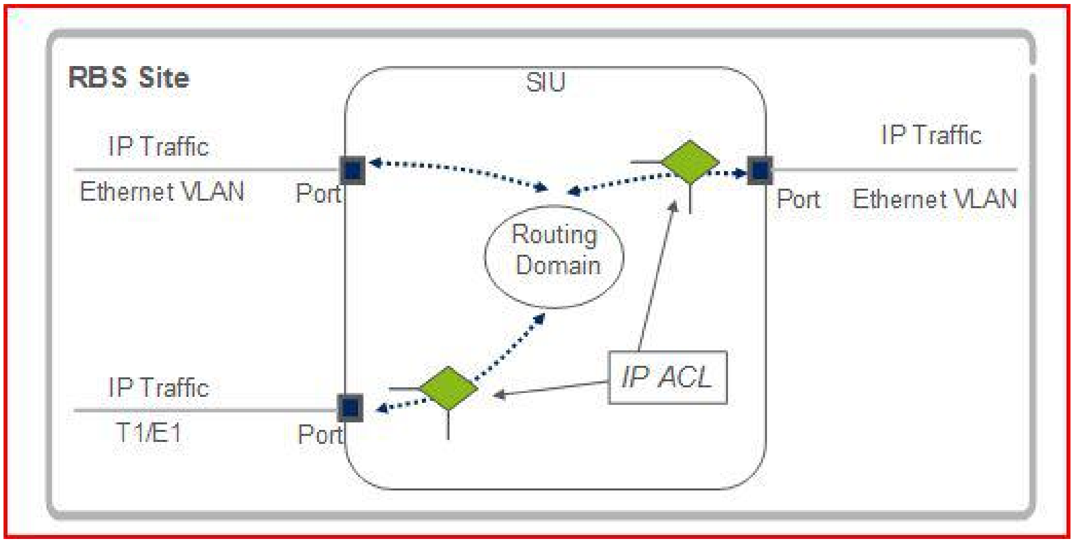
Access Control Lists provide a layer of security to the SIU and transport network by filtering IP traffic according to user-defined rules. The rules define whether an IP packet should be forwarded or dropped depending on source and destination IP addresses, protocol and packet type.

2.9.3 Benefits

Benefits and Operator Value

ACLs are usually applied to the ingress side of the SIU to protect it from malicious attacks and to stop IP traffic from unwanted sources entering the node. They may also be applied to the egress side to prevent the SIU from sending unwanted traffic into the network.

2.9.4 Description



Access Control Lists (ACL) provide protection against external threats to the node and the network by filtering IP-based traffic based on a set of configurable criteria. For the SIU application the ACL consists of a list of up to 64 criteria, each consisting of a "5-tuple" set of terms: source/destination IP address (range), source/destination Port number (range), protocol ID, packet type and an allow/deny instruction for packets matching the criteria.

Packets arriving at the node are inspected against each sequential ACL entry. A packet is allowed to pass as soon as it matches an "allow" entry, so it is recommended that frequently matched entries be placed near the top of the list for speed. If packets are frequently denied for the same reason, a "deny" entry can be placed near the top of the ACL so the unwanted packets are dropped as quickly as possible. If no matching entry is found, the default action is to deny access to the packet and the packet will be dropped.

The approach of denying all packets, except those that are explicitly allowed by the ACL, means that only packets required for the receiving network to operate correctly are permitted.

It is possible to configure up to eight ACLs on the SIU. Each IP interface can be associated with one ACL, but each ACL can be associated with more than one IP interface, provided their requirements are the same.

2.10 Multiple Uplinks

Feature Identity:	FAJ 121 1850/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

2.10.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.10.2 Summary

Commercial Attention: feature FAJ 121 0677/1, IP over E1/T1, is optional in the TCU/SIU. It is required if multiple uplinks including IP over E1/T1 are to be implemented.

Multiple uplink interfaces are available at the TCU/SIU to enable several IP/Ethernet connections, or different forms of transport, such as IP over Ethernet and IP over E1/T1, to be used simultaneously between the TCU/SIU and switching site.

2.10.3 Benefits

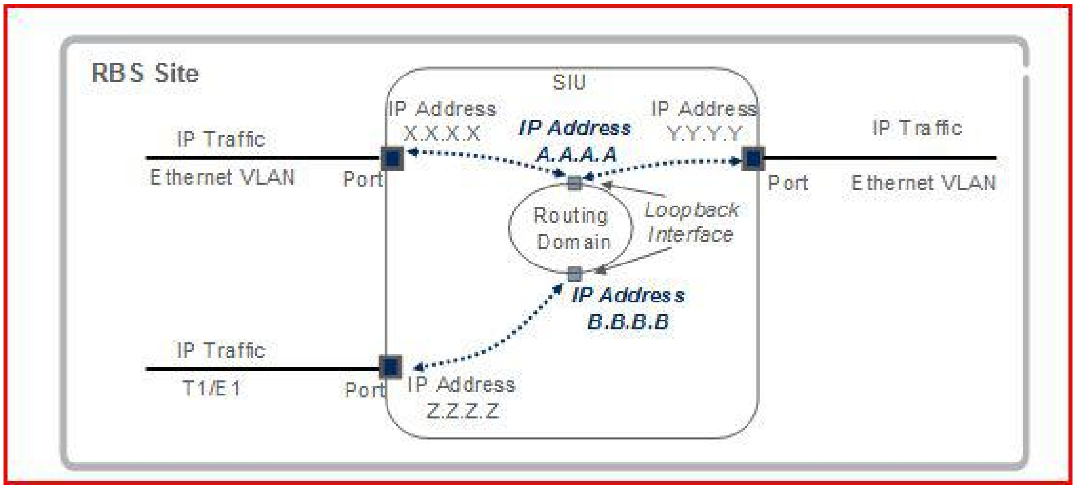
The availability of multiple transport links at one RBS site means that operators can deploy additional transport links either using the same or a different transport technology. This can be used in various ways, for example to implement a high availability service with redundant Ethernet paths between the RBS site and switching site, or to prepare for a smooth transition from IP over E1/T1 to IP/Ethernet.

Taking the example of transport migration, IP/Ethernet transport can be introduced on a planned step-by-step basis by running the existing TDM (IP over E1/T1) transport network and new IP/Ethernet connections simultaneously. For example, an operator may wish to introduce IP/Ethernet for new data services without disturbing an existing IP over E1/T1-based network that primarily handles voice traffic.

This allows maximum use to be made of the legacy network, eases the introduction of Ethernet and prepares for an eventual migration to an all-IP/Ethernet transport regime.

The availability of alternative transport links is a requirement for basic resilience, which was described as part of FAJ 121 0907/1, Bidirectional Forwarding Detection.

2.10.4 Description



The SIU 02 hardware accommodates sixteen E1/T1 connections, eight are available on TCU 02, and both also have eight 10/100/1000 speed, RJ45 electrical ports, four of them combined with SFP ports. These can be allocated flexibly between transport network links, connections to RBSs and Site LAN applications.

The **E1/T1 ports** are shared as needed between connections to RBSs and WAN. They may be combined into ML-PPP bundles either for WAN or CDMA RBS applications. The maximum size of an ML-PPP bundle is eight E1 or T1 links. Typical use cases would result in four or eight links being used for a WAN ML-PPP bundle, two or four bundled for each CDMA RBS, and one or two non-bundled links being used for each GSM RBS.

Up to **eight Ethernet ports** can be configured in total; a maximum of four optical (SFP) ports with the remainder (i.e. four or more) being electrical RJ45 connections.

A typical IP/Ethernet implementation would allocate one or two ports to the WAN, leaving the remaining ports available for WCDMA or LTE RBSs or Site LAN equipment. Where more than one Ethernet port is allocated to the WAN, each is attached to a different VLAN and static route to the switching site.

The configuration of connections can be easily changed as requirements evolve. For example, if a transition is made to an all-IP/Ethernet transport network, the E1/T1 links previously used for IP over E1/T1 WAN can be re-used to connect further GSM or CDMA RBSs.

2.11 Remote System Logging

Feature Identity:	FAJ 121 4041/1, Rev. A
Feature Type:	Basic in T14B
Technology:	

2.11.1 Attention

Commercial attention

Not applicable

Dependencies

No external technical dependencies have been defined for this Feature

2.11.2 Summary

The feature provides the oportunity to collect system logs at central locations for analysis of system perfiormance. The standard format allows for usage of a wide range of tools for this analysis.

2.11.3 Benefits

The feature makes it possible for the operators to efficiently follow and analyse the status of the SIU/TCU nodes, thus supporting efficient operation of the network.

2.11.4 Description

The Remote System Logging feature makes it possible to collect the system log from SIU/TCU and for log messages to be sent from SIU/TCU to remote servers. Up to 5 designated syslog servers can be defined.

The feature supports reliable log transfer to redundant servers and ability to set secure logging through TLS. Data volumes and easy visibility can be selected controlled by using the possibility to filter and classification based on content or severity.

Logs can be selected to be in either a SIU/TCU legacy format or according to standard RFC 5424.

2.11.4.1 Standards

Relevant parts of:, IETF RFC 5424, IETF RFC 5425, IETF RFC 5426, legacy format is based on RFC 3164.

2.12 Site LAN

Feature Identity:	FAJ 121 0703/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	

2.12.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.12.2 Summary

Summary

The Site LAN feature, introduced in SIU SW 09A, allows management equipment to be securely connected to local ports on the SIU. Examples of this are alarm systems and surveillance equipment.

2.12.3 Benefits

Benefits

Modern site equipment normally uses IP and Ethernet technology to communicate with central management systems. The Site LAN feature allows such products to be installed on-site without the need for any extra equipment or dedicated backhaul capacity. The activation and deactivation of the ports and connectivity are controlled byOSSto enhance the security level for the RBS site.

2.12.4 Description

Description

The feature enables Site LAN equipment to be connected to Ethernet ports on the SIU. The ports and their connectivity attributes are invoked through OSScommands. Each port used for Site LAN is assigned an IP address and a Subnet Mask. The Subnet Mask defines the number of IP addressable equipment that can be connected to one Site LAN port. All ports are individual IP Subnets. There is no layer 2 connectivity between the ports, as shown in the figure below.

The SIU supports QoS functionality including policing, queuing and scheduling for WAN and Site LAN interfaces. The Diffserv Code point is by default set to the lowest priority for Site LAN traffic to ensure that it does not intrude on the RAN traffic.

The SIU uses a default gateway for outgoing traffic. The routing table will be set up automatically, based on the local subnets and the interfaces to which they are assigned.

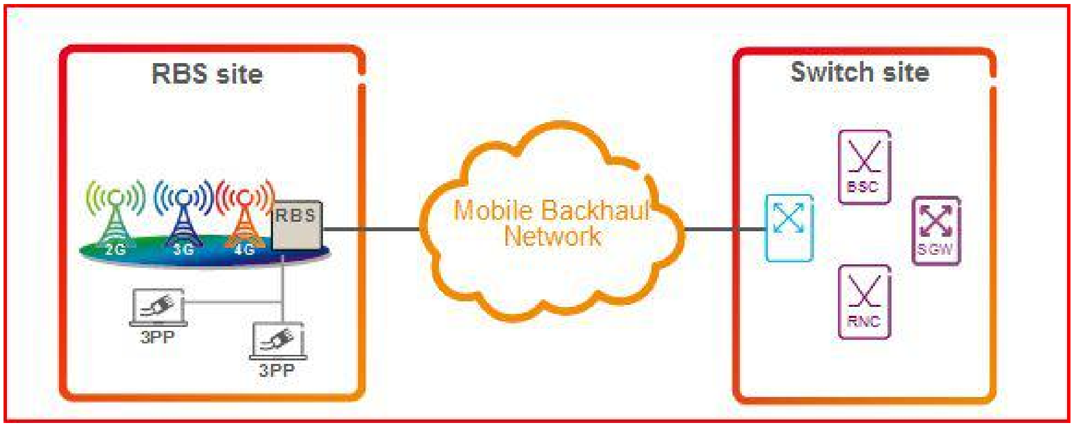


Figure 9 - Site LAN

2.13 STN Local Port Security

Feature Identity:	FAJ 121 0756/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	

2.13.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.13.2 Summary

Summary

TheSTNLocalPortcan be enabled with a manual override procedure whereby On Site Personnel (OSP) can encrypt node sensitive data when it is stored on disk. When the data has been encrypted it cannot be unencrypted except by resetting to factory default settings.

2.13.3 Benefits

Benefits

The override procedure for the local terminal makes it possible for OSP to locally access an STN node whenOSSlost contact with the node, due to link failure or mis-configuration. Encryption of sensitive configuration data makes it harder for an intruder to disturb the radio access network by simulating a node's behavior with stolen configuration data.

2.13.4 Description

Description

Manual operation of the physical layer for theLocalPortand time supervision are used to check whether the node hasOSSconnectivity. If there is no connectivity theLocalPortis enabled and made ready for user-id and password entry for a limited time. If the operator logs on successfully the node restarts with factory settings and is ready to be configured from theLocalPort.Log on failure results in alarms and disabling of theLocalPort.

The AES-Rijdael standard is used for encryption, in which a CLI command is used to generate a random encryption key. The key cannot be changed - it is only possible to revert the system to clear-text by using a command to reset it to factory settings.

2.14 System Improvements in SIU T14A

Feature Identity:	FAJ 121 3781/1, Rev. A
Feature Type:	Basic in T14A, T14B
Technology:	

2.14.1 Attention

Commercial attention

Not applicable

Dependencies

No technical dependencies have been defined for this Feature

2.14.2 Summary

Control of FM and PM Subscriptions via the MOM

In T13B and earlier releases, the FM subscriptions and the PM measurement can be configured with a combination of MO attributes and STN CLI commands. This System Improvement allows it to be fully controlled via MO attributes.

Updates to the subscriptions done via legacy subscription command will result in corresponding updates to the subscriptions in the MOM, i.e. it will be stored and be visible in the MOM. Vice versa, updates to subscription via the MOM will be visible via legacy subscription commands.

Debug Command to Get Ethernet Port Status

Debug command for reading detailed status and debug information for Ethernet ports and SFP Modules. This command is useful when debugging problems related to Ethernet ports and SFP Modules.

Debug Command to Reset Counters

Debug command for resetting one or more counters.

This command is useful in relation to test and debugging.

Configured Scheduler Mean Rate Available as PM Data

The configured Scheduler Mean Rate of a traffic manager is made available as PM data.

Including the Scheduler Mean Rate in the PM data allows KPI tools like ENIQ, which otherwise does not have access to the configured Scheduler Mean Rate, to calculate the bandwidth utilization.

Performance Report Messaging (PRMs) on FDL according to ANSI T1.403

Makes is possible to enable transmission of Performance Report Messaging (PRM) on the Facility Data Link (FDL) on a T1 port.

The FDL channel is carried by the framing bits, so it will not consume payload bandwidth.

This will enable the operator to read T1 receive status from the SIU via peer equipment that supports PRM over FDL.

Command to Approve SW and Configuration after the Verification Period

Command to approve the running SW and configuration.

Issuing this command will copy the running SW and configuration to the backup areas, which will be used in the event of a roll-back.

This command should be issued by the operator after the verification period following an SW and/or configuration upgrade. This will ensure that the system will have a valid configuration in the event of a roll-back to the backup SW and configuration.

2.14.3 Benefits

The main benefits are in the monitoring and fault finding areas. See under overview.

2.14.4 Description

Se under overview.

2.15 System Improvements in SIU T14B

Feature Identity: FAJ 121 4034/1, Rev. A

Feature Type: Basic in T14B

Technology:

2.15.1 Attention

Commercial attention

Not applicable

Dependencies

This Feature has no dependencies.

2.15.2 Summary

Support of /31 (RFC3021) Subnets

The purpose of configuring /31 subnets is to conserve IP addresses. The number of allocated IP addresses per point-to-point link can be halved from 4 to 2.

The 'Support of /31 (RFC3021) Subnets' system improvement makes it possible to configure a subnet for an IPv4 interface with a prefix length of 31 bit.

A prefix length of 31 bit is configured via the Managed Object Model in a same way as shorter prefix lengths (i.e. of 30 bit and less) are configured.

Routing Loop Prevention by Specifying a Null Route

Null Routes can be used to avoid routing loops that can otherwise occur if a route gets inactive. The basic functionality of a Null Route is to intentionally reroute a packet to a Null interface (also known as a sinkhole or blackhole) so that the reply packets do not go out of the device.

The system improvement makes it possible to configure an IPv4 null route. Packet destined to a Null Route will be discarded.

Whenever a routing protocol summarizes routes, this means that the router might receive traffic for any IP address within that summary. Because not all IP addresses are always in use, there is a risk of looping packets in case default routes are used on the router which receives the traffic for the summary.

Null routing can also be used to filter out traffic destined to a certain address. It has an advantage over Access Control Lists (ACL) since it has virtually no performance impact, Null Routing can often sustain higher throughput than ACL filtering. For this reason, Null Routes are often used to mitigate denial-of-service attacks before the packets reach a bottleneck.

Ethernet Port Mirroring

With the purpose of troubleshooting, it is possible to get all traffic on an Ethernet port mirrored to some external test equipment.

The 'Ethernet Port Mirroring' system improvement makes is possible to get all traffic on an Ethernet port duplicated and sent out on another dedicated Ethernet port.

All Ethernet frames received and transmitted on a selected source port is duplicated and transmitted on a selected destination port. The mirroring will take place with line speed.

Only one source port and one destination port is supported. The source port and the destination port can be selected freely among the external Ethernet ports. The destination port will be reserved for the mirroring function and cannot be used for normal traffic while port mirroring is enabled.

Port mirroring is configured via the Managed Object Model.

2.15.3 Benefits

See under Overview

2.15.4 Description

See under Overview

2.16 Transport Sharing

Feature Identity:	FAJ 121 0702/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE, ETSI, ANSI, Wireless Broadband, GRAN, TD-SCDMA

2.16.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.16.2 Summary

This feature allows backhaul capacity to be shared between different types of traffic (GSM, WCDMA, CDMA and LTE). This feature was initially introduced for GSM and WCDMA only in BSS 08A.

Commercial Attention: feature FAJ 121 0677/1, IP over E1/T1, is optional in the SIU/TCU. It is required if the IP over E1/T1 transport mentioned in this section is to be implemented.

2.16.3 Benefits

When WCDMA traffic is added to an existing GSM infrastructure, the backhaul capacity requirements increase considerably. A GSM RBS is typically connected with one or two E1/T1s and introducing WCDMA can easily double this capacity requirement. Operators introducing WCDMA to an existing GSM network benefit from sharing the total backhaul capacity between both systems. This solution has several advantages:

- For larger GSM sites the Transport Sharing feature may mean that it is possible to launch a WCDMA service without needing to increase backhaul capacity.
- During off-peak hours the combined backhaul capacity can be used for Packet Data services like HSPA. Consequently the launch of HSPA with peak capacity specifications is more economical.
- The Ericsson Transport Sharing feature is based on an All-IP technology making the solution future-proof for all services. This simplifies the introduction of Edge Evolution, Evolved HSPA and later on LTE based services.
- The solution can initially be based on IP over E1/T1 technology. When, IP/Ethernet based services are subsequently introduced (for example, when launching HSPA), migration to Ethernet transport is greatly simplified.

Value to Operators

The main operator value is the reduced cost for backhaul when introducing WCDMA networks in an existing Ericsson GSM network, specifically when only leased PDH (E1/T1) transmission is available. Usually the E1/T1 circuits are expensive and the operators have entered into supply contracts lasting several years so it is essential to use them as fully as possible. Using the transport sharing feature the backhaul bandwidth can be shared between GSM and WCDMA, reducing the need to increase the number of E1/T1s.

Operators who have implemented IP over Ethernet transport, either with a self-built network (such as Ericsson Mobile Backhaul) or using leased capacity, also benefit from transport sharing to fully exploit the available bandwidth. Transport sharing is also an essential feature for modern, multi-standard RBSs (such as Ericsson RBS 6000), which bring numerous benefits including reduced footprint and power consumption at the RBS site.

2.16.4 Description

The sharing solution is based on the SIU/TCU's ability to aggregate many traffic types (GSM, WCDMA, LTE and CDMA) and, if applicable, Site LAN traffic over a single backhaul link. See Figure 8 below.

The SIU/TCU site router aggregates Abis IP and Iub IP traffic over the WAN port on the SIU/TCU. Traffic is prioritized based on DiffServ code points. It is essential that the priorities and queue depth in the SIU/TCU be configured correctly to maintain the quality of RAN services.

If the backhaul technology is E1/T1 instead of IP/Ethernet the optional IP over E1/T1 feature is required (see FAJ 121 0677/3, IP over E1/T1). In this case the SIU/TCU uses IP over E1/T1 on the legacy TDM leased lines, enabled using ML-PPP. One or several of the 16 E1/T1 ports available on the SIU/TCU will be used for backhaul. A router at the switching site is needed to terminate the ML-PPP bundles and route the IP packets to the BSC and RNC. This function has been verified with both SmartEdge and Tellabs products.

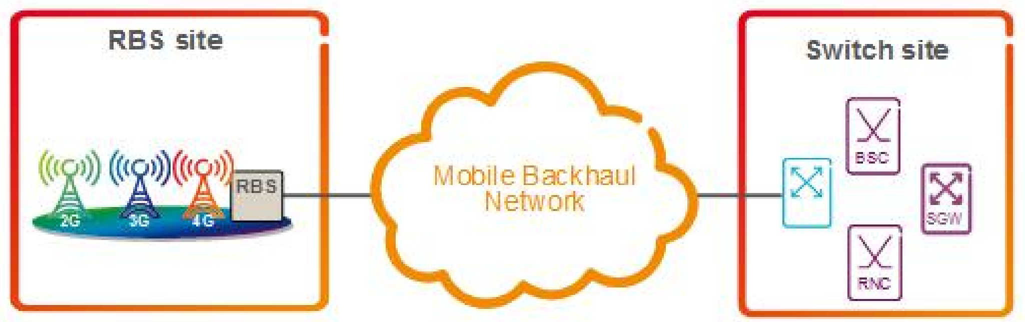


Figure 8 Transport Sharing

2.17 VLAN

Feature Identity:	FAJ 121 0704/1, Rev. A
Feature Type:	Basic in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE, Fixed Broadband

2.17.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

2.17.2 Summary

This feature introduces the ability to configure Virtual Local Area Networks (VLANs) on the TCU/SIU Ethernet ports.

2.17.3 Benefits

Traffic using the Mobile Transport Network may be separated by using a different Virtual LAN (VLAN) for each traffic type or mobile technology. VLANs are a transport resource that can be used to provide traffic segregation for security, performance, traffic engineering, Quality of Service (QoS) marking using standard Priority Code Point (PCP) values, and logical segmentation of site equipment and services.

The figure below illustrates where VLANs are defined for each mobile technology at an RBS site. This puts each mobile technology into a separate broadcast domain. These can be managed separately for traffic separation and QoS handling in the Transport Network.

2.17.4 Description

The VLAN tagging capability on the TCU/SIU provides an IEEE 802.1Q standards- compliant method by which to separate traffic in the RBS site and Mobile Transport Network using Customer VLANs (C-VLAN).

The following configuration options are available:

- The TCU/SIU supports up to 256 C-VLANs, which are treated as shared resources that can be configured on the Ethernet ports.
- Any VLAN ID between 0 and 4094 may be configured on any Ethernet port.
- Supports configuration of a single VLAN ID for Abis over IP traffic and NTP synchronization traffic.
- The management interface may be configured with a VLAN ID.
- Configurable global mapping table for DiffServ Code Point (DSCP) to PCP.
- Configurable global mapping table for DSCP to egress queues.
- Mapping of DSCP to PCP is performed on egress traffic.
- Manually configurable IP routes using a global routing table.
- The Traffic Manager may be configured to shape traffic based on IP packets or Ethernet frames.
- The Traffic Manager supports up to eight egress queues.

2.17.4.1 Standards

IEEE 802.1Q

3 General - OPTIONAL FEATURES

3.1 Centralized User Management

Feature Identity: FAJ 121 4039/1, Rev. A

Feature Type: Optional in T14B

Technology:

3.1.1 Attention

Commercial attention

Requires OSS-RC Single sign in server and Autentication and Autorisation servers. If encryption with SSL is used, the PKI/CA support in OSS- RC needs to be available.

Dependencies

No technical dependencies have been defined for this Feature

3.1.2 Summary

The Centralized User Management feature introduce support for using the centralized Single Log-on Server in OSS-RC, giving a centralized point of authentication and authorization (AA), when logging in to the SIU. In addition the feature enables personal user accounts (username and password) to be set up on the remote servers.

3.1.3 Benefits

The feature provides user authentication for the command line interface using a remote Authentication and Authorization (AA) server that enables auditing of user activity for personal accountability.

This is done by adding support in the node for using the Single Log on Server and centralized point of authentication and authorization (AA servers) in the OSS-RC.

The central authentication gives stronger password rules as well as the possibility to limit the user access to up to three configurable attributes, e.g. land, region, radio technology or other customer specified.

In addition personal accounts (username and password) can set up on the remote servers on OSS-RC, allowing for individual user names and passwords at login.

3.1.4 Description

The feature provides user authentication for the command line interface using a remote Authentication and Authorization (AA) server that enables auditing of user activity for personal accountability, when logon to the SIU. The "Lightweight Directory Access Protocol" (LDAP) is used for accessing the (AA) server.

Personal accounts (username and password) can set up on the remote servers on OSS-RC, allowing for individual user names and passwords at login. In terms of access control profiles only user access profile (admin) is currently supported.

Centralized User Management means that user credentials (username, password) are checked towards a remote Authentication and Authorization (AA) server located at the OSS-RC. The Centralized User Management feature can be deployed with one or two Authentication and Authorization (AA) servers.

The feature supports secure LDAP over SSL (Secure Socket Layer) as well as unencrypted LDAP. The SSL encryption uses a public-and-private key system. If the SSL encryption is uses it requires Public Key Infrastructure (PKI)/ Certificate Authority (CA) support in the OSS-RC, for digital certificate handling. The SCEP (simple certificate enrolment protocol) is supported for download certificate for LDAP over SSL.

The first time Centralized User Management is activated, some preparations must be done in OSS RC.

3.2 Real- time Security event logging

Feature Identity:	FAJ 121 4038/1, Rev. A
Feature Type:	Optional in T14B
Technology:	

3.2.1 Attention

Commercial attention

Not applicable

Dependencies

No technical dependencies have been defined for this Feature

3.2.2 Summary

Network Elements provide logging of security related information.
Using this feature, it is possible to identify and log "security related events" to a centralized log server. Detection and reporting of the events is done in real-time and the events can be transported to the centralized server in a secure way.
The logs can as well be kept on the Network Elements (NE) for a limited time, to be looked at on a per need basis.

3.2.3 Benefits

Identification and detection of unwanted access in the network is needed to prevent and counter unauthorized use and attacks. This feature will help operators to be aware of their network behaviour and provide early warning in order to operators to implement mitigations controls to reduce the effect of attacks from outside parties.

3.2.4 Description

The Network Elements provides logging of security related information in the node.

The purpose of this feature is to provide security events in real-time and allow for the triage of security breaches and assist the application of counter measures to stop threats in progress. The syslog server may be integrated with an additional system, such as a Network Intrusion Detection system, to analyse security events.

Using this feature, it is possible to identify and log "security related events" to a centralized log server. Detection and reporting of the events is done in real-time and the events are transported to the centralized server in a secure way. The logs can as well be kept on the Network Elements (NE) and are looked at on a per need basis. The feature adds support for secure transmission of real time syslog messages to up to 5 remote syslog servers in addition to local logging on node.

In addition, to improve the identification and reaction time of a potential security breach it is recommended to capture and report security events across all Network Elements to a common syslog server

3.2.4.1 Standards

Relevant parts of:, IETF RFC 5424, IETF RFC 5425, IETF RFC 5426, legacy format is based on RFC 3164.

4 IPv6 Package - OPTIONAL FEATURES

4.1 DHCP Relay for IPv6 in SIU/TCU

Feature Identity:	FAJ 121 2968/1, Rev. B
Feature Type:	Basic in T13B, Optional in T14A, T14B
Technology:	WCDMA, LTE

4.1.1 Attention

Commercial attention

Not applicable

Dependencies

The following feature is always required:

- TCU02/SIU02 SW: FAJ 121 2548 - IPv6 Basic Functionality

4.1.2 Summary

The DHCP relay over IPv6 feature enables the SIU/TCU to provide DHCP services to connected IP enabled RBSs and other equipment.

The main use case is to support the auto installation features in WCDMA and LTE RBSs.

4.1.3 Benefits

The customer benefit is the ability to provide DHCP services to the RBS site when IPv6 backhaul is used.

The feature is primarily intended to be used with the RBS auto integration features for WCDMA and LTE RBSs, but it can also be used to provide DHCP services to arbitrary equipment at the RBS site.

4.1.4 Description

DHCP requests from equipment on the RBS site will be forwarded to a DHCP server, typically in the OSS-RC.

4.2 IPv6 Basic Functionality

Feature Identity:	FAJ 121 2548/2, Rev. A
Feature Type:	Undefined in T11B, Optional in T13B, T14A, T14B
Technology:	LTE

4.2.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

4.2.2 Summary

The IPv6 basic functionality feature provides a basic set of functions that makes it possible to use IPv6 to connect the to the TCU/SIU. It includes support for IPv6 static routes with BFD for IP/Ethernet and dual stack implementations, with both IPv4 and IPv6 running alongside each other, as well as certain OAM functions.

4.2.3 Benefits

IPv6 offers a much larger address space than IPv4, and can therefore be useful especially in very large networks in order to avoid complicated replanning of IPv4 address plans when the network is growing.

In networks addressing large numbers of end users, such as fixed broadband access networks, IPv6 provides necessary address space. IPv6 in the Radio Access Networks will simplify sharing the backhaul between fixed and mobile broadband.

4.2.4 Description

The TCU/SIU supports IPv6 on its Ethernet interfaces. Many of the same features are available for IPv6 as for IPv4, for example VLAN support and QoS based on DSCP with mapping to eight queues. Resilience is provided by the availability of several uplink ports supported by the BFD-based failover mechanism.

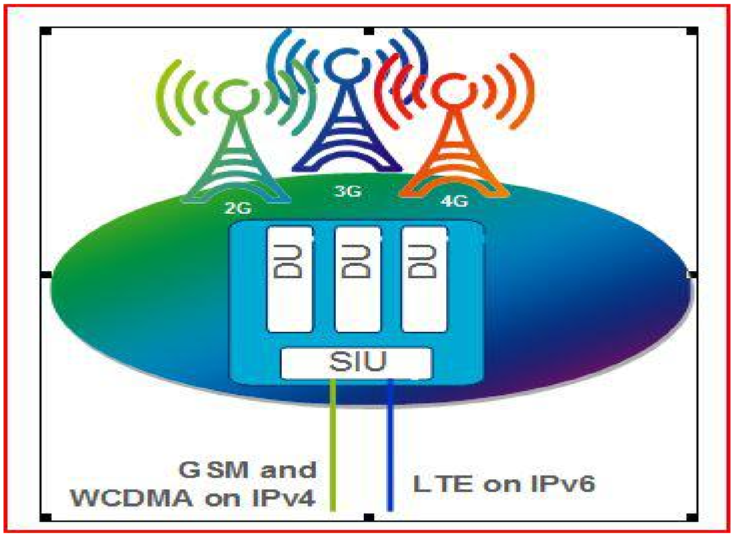


Figure Dual stack IPv4 and IPv6 implementation

A smooth migration to IPv6 is provided by a dual stack implementation, e.g. GSM and WCDMA RANs can continue to use IPv4 while LTE is introduced using IPv6.

OAM functions available for IPv6 include ICMP Echo continuity testing and trace route.

The IPv6 feature supports transmission of IPv6 packets over Ethernet networks, an IPv6 address architecture, ICMPv6, Neighbor Discovery (ND), and Duplicate Address Detection (DAD).

The current implementation of IPv6 support the following functionality:

- IPv6 interfaces.

- Virtual IPv6 interfaces.

- IPv6 static routes together with BFD over IPv6.

- IPv6 bridging.

- VLAN.

- O&M via CLI of Software Management (SM), Configuration Management (CM), and Performance Management (PM).

4.2.5 Enhancement

NTP over IPv6 is supported for the system clock.

SNMP traps are supported. The main usage is for connection to OSS RC.

5 Network Frequency Synchronization Package - OPTIONAL FEATURES

5.1 1588v2 Transparent Clock

Feature Identity:	FAJ 121 2547/1, Rev. A
Feature Type:	Optional in T12A, T12B, T13B, T14A, T14B
Technology:	WCDMA, LTE

5.1.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

5.1.2 Summary

The Transparent Clock (TC) according to IEEE1588v2 allows PTP packets to pass through the TCU/SIU with minimal inaccuracy added. This is essential in applications requiring very strict time synchronization, such as TD-LTE networks (which require timing accuracy in the order of 1.5 micro seconds at the air interface) .

PTP over Ethernet is supported.

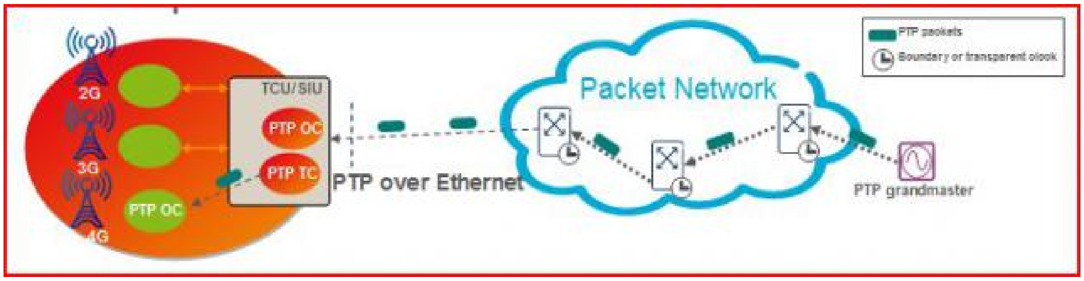
5.1.3 Benefits

Very accurate time synchronization can be achieved using PTP distributed via a RAN packet backhaul network, with TCUs in the synchronization path. PTP offers a cost efficient alternative to GPS.

5.1.4 Description

For distribution of high accuracy time via the packet network, each node in the synchronization path has to contribute minimal inaccuracy to the time stamps. In addition to the standard PTP time server, nodes within the transport network therefore have to compensate for delays normally induced in switches and routers. The Transparent Clock feature modifies the PTP timestamps to account for the variable lengths of time the messages take to traverse the TCU/SIU.

In this way accurate time and phase synchronization signals are provided to network equipment, including the RBS.



The PTP packets pass transparently through the TCU/SIU, with only the modification of the time stamp. The oscillator, or any other synchronization functionality in the TCU/SIU, is involved.

PTP mapping on Ethernet is supported (notice; not PTP/UDP/IP).

5.2 Frequency Synchronization Client with PTP over IP

Feature Identity:	FAJ 121 0683/4, Rev. A
Feature Type:	Optional in T14B
Technology:	GSM, WCDMA, LTE

5.2.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

5.2.2 Summary

This feature enables frequency synchronization using Precision Time Protocol (IEEE 1588v2) for an SIU/TCU connected via a non-synchronous network (e.g. Ethernet). The feature provides the Sync Client in SIU/TCU. This feature enables the SIU/TCU clock to calibrate with an accuracy that allows connected RBSs to generate radio frequency with accuracy according to 3GPP specification (less than 50ppb deviation). The feature offers an alternative to NTP as synchronization protocol.

5.2.3 Benefits

This feature enables clock frequency synchronization of the SIU/TCU using the standard IEEE 1588v2 PTP protocol over a packet backhaul network. No synchronization support from the backhaul network or synchronization equipment at RBS site is required, which makes implementation cost efficient.

5.2.4 Description

The SIU/TCU supports two alternative protocols for getting frequency synchronization information over (non-synchronous) packet networks - NTP and PTP. The basic architecture, method and characteristics are similar.

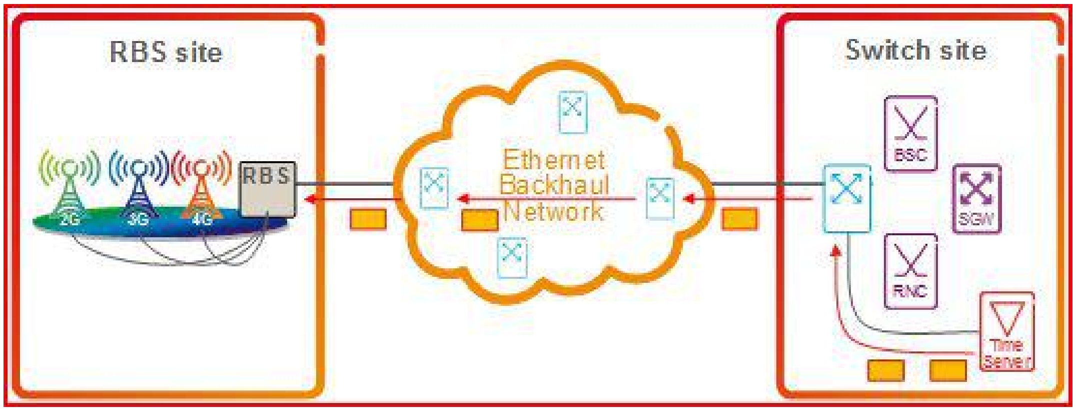


Figure: Frequency Synchronization with PTP over IP

In the Frequency Synchronization client with PTP over IP feature, frequency synchronization for an SIU/TCU is achieved by aligning the frequency of the SIU/TCU to the frequency of an IEEE 1588v2 PTP Master with traceability to a G.811 source.

An Ericsson patented algorithm in the Sync Client filters out the time information and calibrates the SIU/TCU clock. Thereby the SIU/TCU clock supports a radio frequency deviation of less than 50ppb. The timing function generates accurate and stable frequency reference signals to the output interfaces.

The Sync Client in the SIU/TCU initiates an association with the PTP Master by requesting subscriptions of unicast messages. When the subscription has been granted, the PTP Master starts sending Sync messages to the SIU/TCU. The rate of PTP requests will be in the range of one per ten seconds.

The Packet Delay (PD) and packet delay variation (PDV) in the access network between the NTP server and the NTP client in the SIU/TCU is in practice less important because of the long filtering time used for frequency synchronization, provided the SIU/TCU has been synchronized within the last 4 months and any high PDV situation does not persist long-term.

A faster algorithm is used for initial calibration. This faster algorithm is used for initial calibration when the backhaul network is good enough (low enough packet delay variation). If the PDV is too large for the fast algorithm, the calibration will fall back to using the slow algorithm.

The feature requires access to a PTP synchronization server. A SIU/TCU can have up to 6 PTP Masters associated with it for redundancy, but only one is used at any given point in time. The synchronization references are required to have a long term frequency accuracy of better than 10-11, i.e. traceable to a PRC (compliant with ITU-T G.811).

The set of accepted master clockClasses used for frequency synchronization is extended to be fully in line with the Telecom Profile. clockClasses â □¤14, 80, 82 84, 86 and 90 are supported.

5.2.4.1 Standards

IEEE1588v2 Telecom Profile for Frequency (G.8265.1)

5.2.5 Enhancement

The enhancement enables the faster algorithm for initial calibration also after sync server re-selection (only applicable the first time after restart). This reselection could for instance take place if the synchronization server with highest priority is not available at startup of the SIU/TCU.

5.3 Synchronous Ethernet

Feature Identity:	FAJ 121 0913/2, Rev. C
Feature Type:	Optional in T13B, T14A, T14B
Technology:	WCDMA, LTE

5.3.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

5.3.2 Summary

This feature provides support for frequency synchronization of the RBS using Synchronous Ethernet (SyncE). Synchronization sources are placed within the Ethernet Transport network to support sychronization of RBSs using Transport network links.

5.3.3 Benefits

SyncE provides support for frequency synchronization of RBSs using physical layer synchronization distribution. The synchronization solution for the RAN will be similar to that used with TDM backhaul.

Synchronous Ethernet has been introduced to provide operators with a further choice for synchronization at the RBS site. Although verified SoIP (NTP) and GPS solutions are already available, some operators are accustomed to obtaining synchronization directly from E1/T1 transmission lines and have expressed a strong wish for a similar solution in Ethernet transport networks. A physical layer Synchronous Ethernet solution is therefore being introduced to complement the existing solutions.

5.3.4 Description

Synchronous Ethernet has been developed to provide physical layer synchronization that is similar to that provided by E1/T1 transport links.

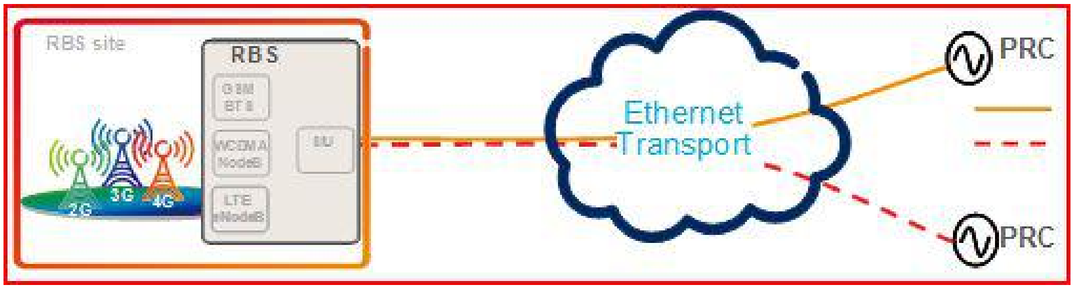


Figure: Overview of Synchronization obtained from Ethernet Transport Network.

Synchronization sources are located within the transport network; these can be used to support frequency synchronization of RBSs equipped with the SIU.

Figure 7 shows how a redundant pair of synchronization servers (Primary Reference Clocks) may be placed in the Ethernet transport network. A maximum of two synch sources are supported.

SyncE is used as a calibration source for the highly stable crystal oscillator (HS-OXCO) in the SIU. The characteristics achieved are similar to those when TDM is used as the calibration source, and the RBS and RBS site configurations supported are the same.

The SIU is configured via its management system to use Synchronous Ethernet. The SIU will always act as a slave in the master-slave synchronized Ethernet network and at least one of its Ethernet interfaces must be configured as a synch slave.

The Synchronization Status Message (SSM) communicates the clock quality level to the SIU. In this way the SIU can select the best available clock source - either one of the two synch servers in the network or its own internal clock. The lowest acceptable quality level is configurable.

The synchronous Ethernet solution complies with applicable parts of ITU-T G.8261, G.8262 and G.8264.

5.3.5 Enhancement

Synchronous Ehternet output with SSM is supported. A primary usage is to distribute frequency to WCDMA and LTE Digital Units, within the RBS or to co-located RBSs. The output characteristics are designed for this usage, and not fully standard compliant.

6 Performance Monitoring Package - OPTIONAL FEATURES

6.1 Ethernet OAM

Feature Identity:	FAJ 121 0909/1, Rev. B
Feature Type:	Optional in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

6.1.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

6.1.2 Summary

Ethernet OAM is used for rapid fault detection and localization as well as performance monitoring on the Ethernet layer. It uses regular Ethernet frames

to troubleshoot end-to-end Ethernet Virtual Connections (EVC), even if these traverse multiple providers. Link OAM is used to detect faults in the link between the SIU/TCU and the first

Ethernet switch in the transport network. It complies with the standard IEEE 802.3ah. Ethernet Connectivity Fault Management (CFM) is used to detect faults in the RAN transport and complies with the standard IEEE 802.1ag. Link OAM and CFM will both generate alarm signals if a fault is found.

Y.1731 Ethernet performance monitoring is used to monitor the delay, delay variation and frame drop rate on an Ethernet service.

6.1.3 Benefits

Link OAM (802.3ah), Ethernet Connectivity Fault Management (802.1ag) and Y.1731 are standards that provides a complete Performance Montoring on an Ethernet layer.

6.1.4 Description

Link OAM

Whereas Ethernet CFM monitors the status of the link from end to end across the transport network and passing several nodes on the way, Link OAM is concerned only with the final link between the User Network Interface - Customer Side (UNI-C) and User Network Interface - Network Side (UNI-N). In this case the UNI-C is considered to be the SIU/TCU and the UNI-N is the first transport network node.

6.1.4.1 Standards

IEEE 802.3ahIEEE 802.1agY.1731

6.2 TWAMP Responder

Feature Identity:	FAJ 121 2549/1, Rev. A
Feature Type:	Optional in T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

6.2.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

6.2.2 Summary

TWAMP is an active method to measure point -to-point IP network performance.

TWAMP defines two sets of protocols: one for setting up performance-measurement sessions, called the control protocol, and another for transmission and reception of performance-measurement probes.

The control protocol enables endpoints to negotiate and start a performance-monitoring session. The protocol for transmission and reception of probes that measure performance defines the packet format that is needed for measuring round-trip performance. This part of the protocol is designed to accommodate hardware-based implementations in order to offload local CPUs during performance-measurement sessions.

The TWAMP architecture is composed of several entities that are responsible for starting the monitoring session and exchanging packets. TWAMP defines different entities for flexibility, and some of them can be collocated for ease of implementation.

The Two-way Active Measurement Protocol (TWAMP) feature performs IP-based performance monitoring of the transport network. It provides the following data:

- Two-way delay
- Delay variation

- Frame Loss
- Availability

6.2.3 Benefits

TWAMP provides operators of large networks a flexible choice of solutions and full visibility into network performance via interoperability among all devices deployed in their networks. It works by measuring core and edge IP performance through cooperation between the routers and switches in the network.

Any two endpoints can interoperate and therefore remove the need for managers to deploy systems with closed proprietary protocols for measuring performance.

TWAMP brings troubleshooting value to personel in Network Operation Centers, as well as providing network trend analysis data for network design engineers.

6.2.4 Description

The figure below outlines how TWAMP is implemented to monitor a transport network.

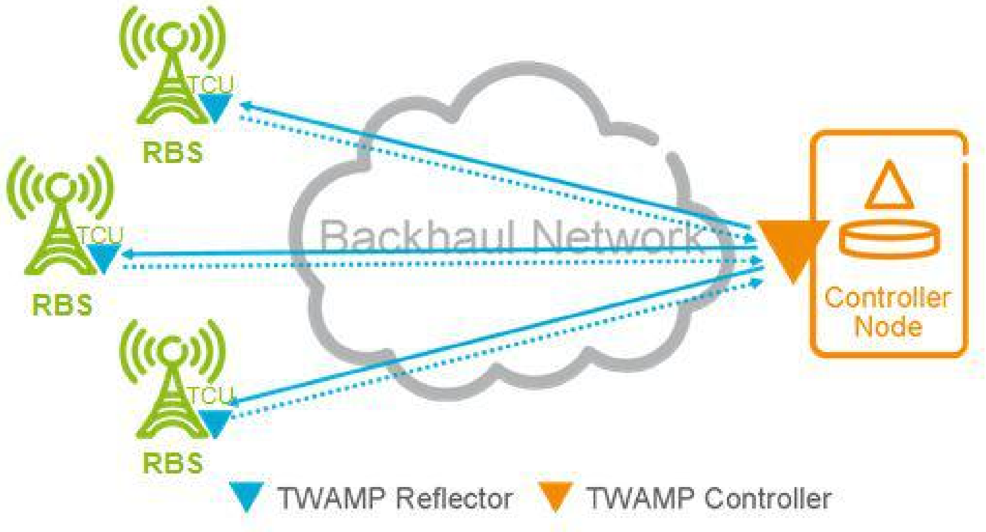


Figure TWAMP implementation

A TWAMP controller node can be deployed at various locations in the network and sends test messages across the transport network to the TCU/SIU. The TCU/SIU is equipped with TWAMP responder software, and the test message is time-stamped before being sent back to the controller node. Returned messages are analyzed to provide the following data:

- Two-way delay
- Delay variation
- Frame Loss
- Availability

TWAMP test messages are based on UDP, and the system works with Ethernet or other IP transport networks. The TWAMP system is fully compliant with IETF RFC 5357.

The IP RAN reference solution documentation provides guidelines on how to design performance monitoring networks using TWAMP.

6.2.4.1 Standards

RFC 5357

6.3 Y.1731 Initiator

Feature Identity:	FAJ 121 3241/1, Rev. A
Feature Type:	Optional in T13B, T14A, T14B
Technology:	

6.3.1 Attention

Commercial attention

Not applicable

Dependencies

No technical dependencies have been defined for this Feature

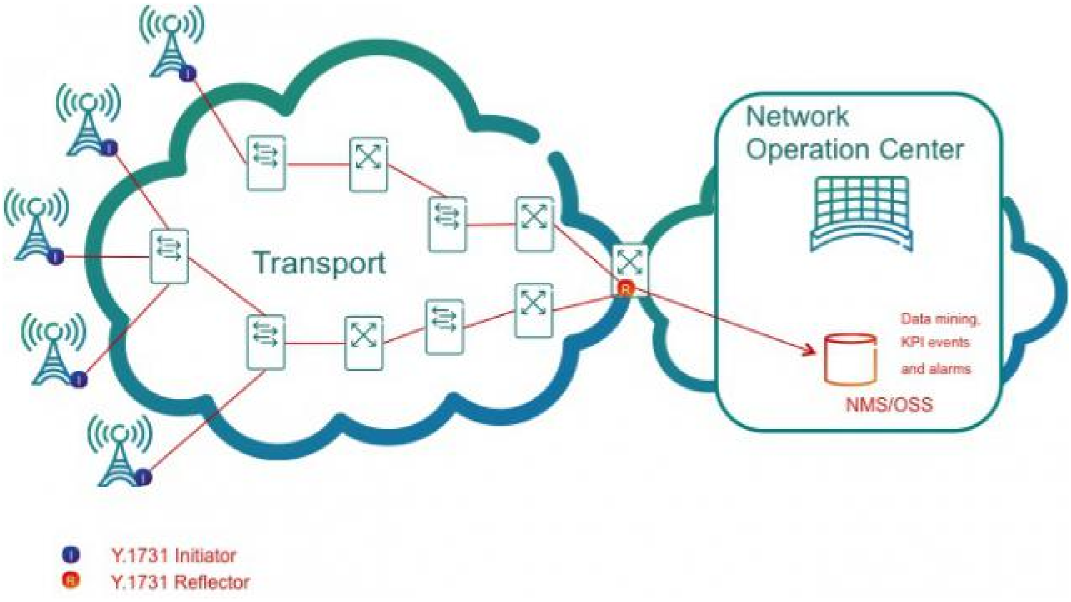
6.3.2 Summary

The "Y.1731 initiator" feature allows the SIU/TCU to act as the initiator for Y.1731 performance monitoring measurements. This feature is a complement to the existing Y.1731 implementation that is a part of the Ethernet OAM solution.

6.3.3 Benefits

By introducing the Y.1731 initiator in the SIU/TCU the Ethernet OAM solution becomes bookended. To have a Y.1731 initiator placed centrally in the network can often be quite expensive. By initiating the Y.1731 measurements from the RBS site and reflect it on the existing router placed at the controller site, this solution will not require any additional product or hardware.

6.3.4 Description



6.3.4.1 Standards

ITU-T Y.1731

7 Routing and Resilience Package - OPTIONAL FEATURES

7.1 Bidirectional Forwarding Detection

Feature Identity:	FAJ 121 0907/1, Rev. A
Feature Type:	Optional in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

7.1.1 Attention

Commercial attention

Commercial attention: It is a prerequisite for this feature, and subsequent features using BFD, that the peer switching site node must also support BFD.

Dependencies

No internal technical dependencies have been defined for this Feature

7.1.2 Summary

Bidirectional Forwarding Detection (BFD) is enabled at the TCU/SIU and the switching site to detect failures between them. Nodes at each end of the IP path send periodic BFD packets. The next IP hop node receives the packets at the same, negotiated interval. If either node stops receiving packets there is assumed to be a fault at some point in the transmission path. In this case IP routing will be used to reroute the traffic.

COMMERCIAL ATTENTION: : It is a prerequisite for this feature, and subsequent features using BFD, that the peer switching site node must also support BFD

Notes:

1 BFD is additional to the existing interface status detection provided by the TCU/SIU.

2 BFD is not supported on IP over E1/T1 interfaces (ML-PPP). The ML-PPP bundle will stay alive provided that at least one component E1/T1 link is active. If the entire ML-PPP bundle fails this will be detected by normal interface monitoring and failover to an alternative path (if available) will follow.

7.1.3 Benefits

BFD allows failures along the IP path between TCU/SIU and switching site to be detected within milliseconds (depending on configured transmission intervals and retry attempts). This facilitates rapid response mechanisms to minimize service disruption.

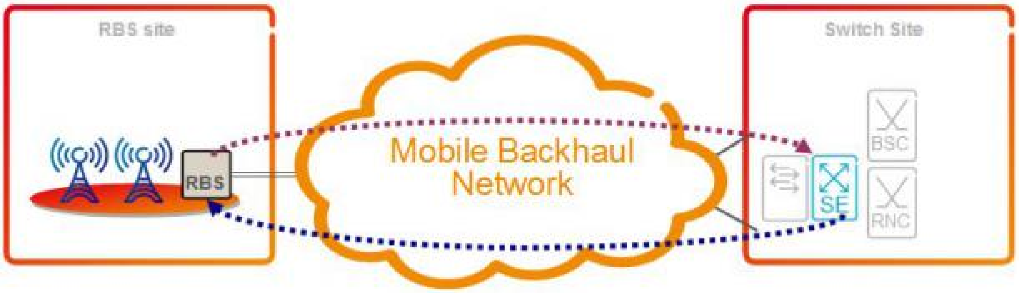
This feature reduces the impact of faults in the network by providing fast detection and fast failover to an alternate path.

This allows traffic to continue flowing with minimal interruption.

7.1.4 Description

Traffic is routed between the TCU/SIU and switching site using static routes. For a given destination there can be more than one static route, using different uplink interfaces and possibly different interface types.

For example, one or two IP/Ethernet WAN links may be available, alongside one IP over E1/T1 (ML-PPP bundle) interface. This would be typical during the migration process from a legacy TDM RAN to IP/Ethernet.



Fault detection
The availability of the Ethernet path between the TCU/SIU and next-hop router at the switching site is monitored using BFD according to RFC 5880.

Periodic BFD packets are sent in both directions between IP interfaces on the TCU/SIU and switching site node. Where multiple Ethernet interfaces are used for the WAN at the RBS site, BFD can be run on all of them.

The BFD packet interval is initially configured at both the TCU/SIU and peer node at the switch site. The interval between packets (both at the send and receive side) can be configured as low as 10ms.

The TCU/SIU and switching site node both monitor the receipt of BFD packets. If either node fails to receive a configurable number (typically between 3 and 5) of packets, some component of the bidirectional path is assumed to have failed and the link is declared down. Thus, the time taken for BFD to detect a failed link can be calculated as:

(number of missed BFD packets +1) * (packet send/receive interval)

If a link failure is detected and the link withdrawn from use, the packet interval is increased to prevent the network being flooded with unneeded BFD packets. This "slow-timer" interval may be configured from one up to several seconds.

BFD packets are assigned to the highest priority queue (EF) allowed for IP traffic. This is necessary to avoid "false" faults being detected due to packet drop in times of network congestion.

IP over E1/T1 links are combined in ML-PPP bundles. The bundle stays connected as long as at least one component link (out of typically 2, 4 or 8 links) remains alive.

The TCU/SIU's electrical circuitry can also detect faults on Ethernet and E1/T1 interfaces. The most typical detected fault is Loss of Signal (LOS), which is when there is no signal on the interface, for example due to a plug being removed.

Failover
If a defective link is detected, all affected static routes are withdrawn from the active Forwarding Information Base (FIB) and traffic is transferred to an alternative link. The new link may be IP over E1/T1 or IP/Ethernet, whichever is available, irrespective of the failed link type. Failovers will be completed within 250ms of the fault being detected.

Recovery
A hold-down timer is used to avoid unnecessary switching between routes, and to ensure that routes being re-established after a failure are fully active before use. After BFD detects that a link has become available again, no traffic shall use that link until the configurable hold-down period has expired. After the timer expires, the route used will revert to that with the lowest-cost metric.

When multiple routes with equal metrics are available to the same destination, traffic will continue using the same route, regardless of the availability of the other equivalent routes.

7.1.4.1 Standards

RFC 5881

7.2 OSPFv2 Dynamic Routing

Feature Identity:	FAJ 121 2545/1, Rev. A
Feature Type:	Optional in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

7.2.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

7.2.2 Summary

Commercial attention: BFD is a separate optional feature FAJ 121 0907

Multiple Uplinks is a basic feature FAJ 121 1850

The introduction of OSPFv2 dynamic routing is a routing capability improvement in the TCU/SIU. In early releases only one route was available between the TCU/SIU and switching site router. In release T11A multiple uplinks and BFD were introduced, giving the TCU/SIU the capability to failover to an alternative (but still static) route in the event of a failure. With dynamic routing based on OSPFv2 the TCU/SIU is able to choose from all available routes, with minimal configuration effort required.

7.2.3 Benefits

OSPFv2 brings flexibility to the network. Multiple network paths are available via OSPF network design. This enables hub sites to have more options to route traffic when comapred to simplier failover scenarios that use only one Primary and one Backup link.

Configuration is simplified for router administrators when compared to traditional static routes.

Reliability is improved as any available route can be used in the event of a failure in the primary transport link when OSPF is used in conjunction with the BFD feature.

7.2.4 Description

The Open Shortest Path First (OSPF) protocol, defined in RFC 2328, is used to distribute routing information within a single Autonomous System (AS). All routers in the AS that support OSPF are known to each other, and the elected Designated Router maintains a list of routers together with all routes between them. Each route is assigned a link cost based on factors such as distance, link availability, throughput and reliability to create a dynamic assignment of traffic to equal-cost paths.

Note: The Designated Router (DR) is always located at the Switching Site; the TCU/SIU do not scale to support this function in OSPF

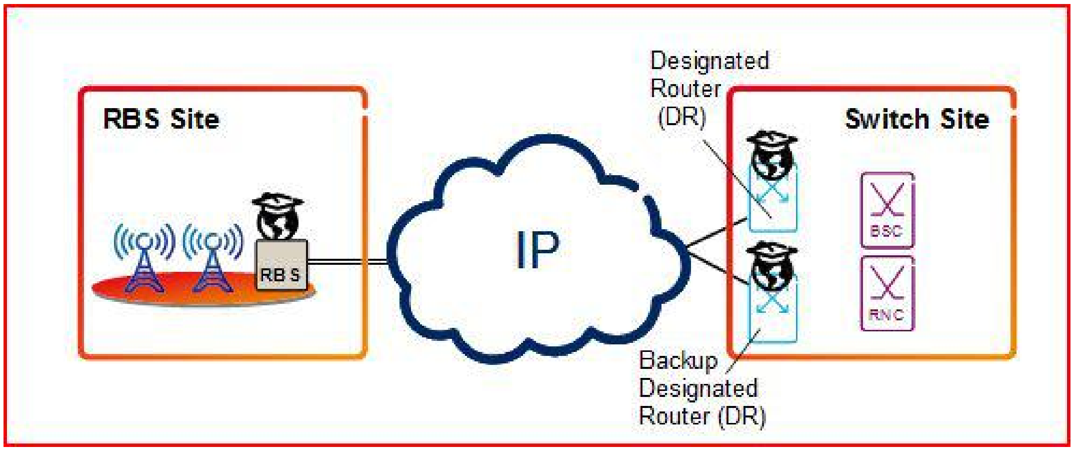


Figure OSPF routers at RBS and Switch sites

OSPF maintains link state information and periodically updates the routing tables held by all routers in the AS, In the event of a link failure, OSPF will remove routes associated with the failed link from the routing table. Traffic will continue flowing using the next lowest-cost route.

OSPF is compatible with Bidirectional Forwarding Detection (BFD). BFD can provide faster information about failures than waiting for them to be discovered by OSPF, so routes can be re-assigned more quickly.

Individual interfaces on the TCU/SIU can be designated passive for OSPF; the TCU/SIU Ethernet interfaces can be completely flexibly allocated to WAN, RBS or Site LAN connection and OSPF is only activated for WAN.

Other OSPF features supported by the TCU/SIU include MD5 authentication, the management tools OSPF logging and MIB, and NSSA (Not-So-Stubby-Area) - a mechanism by which the size of the routing table may be reduced by removing extraneous routes.

7.2.4.1 Standards

RFC 2328

7.3 Policy Based Routing (PBR)

Feature Identity:	FAJ 121 0912/1, Rev. A
Feature Type:	Optional in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, LTE

7.3.1 Attention

Commercial attention

Commercial Attention:
PBR must also be supported and configured on the RAN switch/router at the switching site.

Dependencies

No internal technical dependencies have been defined for this Feature

7.3.2 Summary

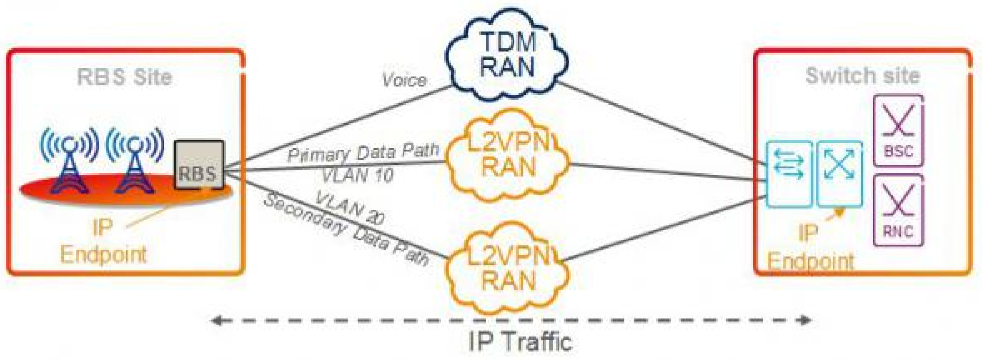
Commercial Attention:
PBR must also be supported and configured on the RAN switch/router at the switching site.

Existing routing methods use only the destination IP address of each packet to determine its route. Policy Based Routing examines a larger set of packet attributes such as protocol type, priority, source/destination address and source/destination ports and uses these in route determination. The route taken by the packet can thus be more finely controlled than with conventional routing.

7.3.3 Benefits

PBR in the TCU/SIU enables the operator to control the route taken to the switching site by specific types of traffic, thus segmenting traffic so that different traffic types use the most appropriate transport networks. For example PBR may be used to ensure that lower priority traffic uses the lowest cost transport resources.

7.3.4 Description



In a conventional routing system the route taken by traffic leaving the TCU/SIU is determined only by its destination IP address.

With policy-based routing a fine-grained routing decision can be made by filtering fields in the IP header and VLAN header of incoming IP packets.

Filtering takes place by matching incoming packets with a set of rules that is configured at the TCU/SIU's ingress interfaces. Each interface can be configured with a different set of rules. The infrastructure used for PBR is an extension of that used for Access Control Lists (basic feature), which simply pass or drop packets according to a similar field list (ACLs do not look for DSCP field matches).

The field list used for filtering consists of the IP 5-tuple set of source/destination addresses, source/destination ports and protocol, together with priority given by Diffserv Code Point (DSCP) or Priority Code Point (PCP, IEEE802.1p p-bit).

If a packet is found to match a rule it will be forwarded according to the action specified.

7.4 QoS Remarking and Policing

Feature Identity:	FAJ 121 3782/1, Rev. A
Feature Type:	Optional in T14A, T14B
Technology:	

7.4.1 Attention

Commercial attention

This feature is a L3 feature, not intended to work on L2

Dependencies

No external technical dependencies have been defined for this Feature

7.4.2 Summary

- The feature is aimed at 3PP nodes within the cell site, which does not support proper marking of originating traffic themselves. The feature will allow that traffic from such nodes is marked in accordance with the classification policy for the network.
- When SIU/TCU aggregates traffic from external systems such as alarm systems, not able set correct DSCP bits, SIU/TCU can re-mark (mark) the incoming traffic.
- Remarking is supported for IPv4
- The feature also includes ingress policing to protect the node from being flooded with traffic from untrusted interfaces, in worst case being remarked as high-priority traffic. A number of policers can be configured. A rate limit and a maximum burst size are configured per policer and excess traffic is dropped

7.4.3 Benefits

Gives the Operator a possibility to connect other devices on the cell site such as alarm equipment and prioritize that traffic according to operators policies

7.4.4 Description

- The QoS Remarking feature allows the operator to configure remarking of incoming packets and frames.

- Remarking is supported for IPv4 forwarded traffic. It is not supported on node local terminating and originating traffic. The remarking is based on incoming IP interface.

- Remarking consists of updating the DSCP value in the IP header. The DSCP value is mapped to the 6 MSB of the Type Of Service field in a IPv4 header.

- The remarking function will be an extension to the existing remarking function.

-The current Remarking function is extended, so it will be possible to specify the DSCP to use for the remarking on an untrusted interface.

- Changes from T13A

-In T13A it is possible to configure that the DSCP of packets coming in on an IP interface should not be trusted. For IP forwarded traffic, the packets from an interface with untrusted DSCP is remarked to DSCP 0 (BE), and node internal PHB for the packet will be accordingly.

-The trust DSCP configuration must in T13A be the same for all IP interfaces connected via VLAN to the same Ethernet interface. It must also be the same for all IP interfaces on top of MLPPP.

-The restrictions that the trust DSCP configuration must in be the same for all IP interfaces on top of VLAN interfaces on the same Ethernet interface and for all IP interfaces on top of MLPPP is removed.

-In T13A it is possible to configure trust DSCP to apply on bridged traffic by configuring a dummy IP interface on top of a dummy VLAN interface on the same Ethernet interface as the VLAN interface used for bridging. This possibility will be removed. If the possibility is still needed, it should be made possible to configure it directly on the VLAN interface used for bridging instead.

The feature also includes ingress policing. A number of policers can be configured. A rate limit and a maximum burst size are configured per policer and excess traffic is dropped. The policer to apply on a packet is selected based on the incoming IP interface.

8 Security Package - OPTIONAL FEATURES

8.1 IPsec client for SIU/TCU

Feature Identity:	FAJ 121 3783/1, Rev. A
Feature Type:	Optional in T14A, T14B
Technology:	GSM

8.1.1 Attention

Commercial attention

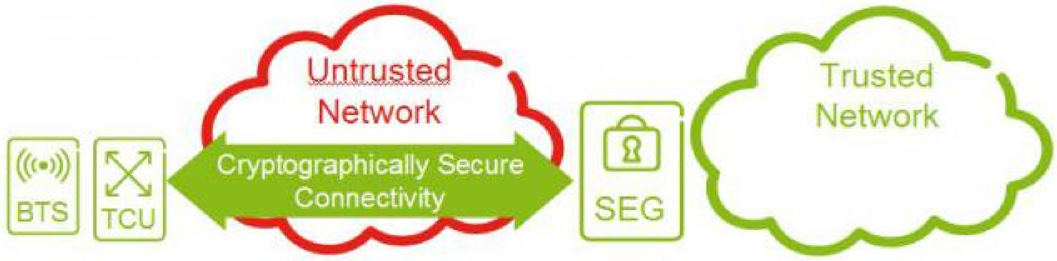
Not applicable

Dependencies

The feature requires a IPsec Security Gateway and PKI infrastructure in case certificate based authentication is used.

8.1.2 Summary

IP Security (IPsec) is an open standard (RFC 4301) that defines a protocol suite for securing IP traffic. The SIU/TCU use IPsec to secure GSM Abis IP and SIU/TCU OAM traffic over a non-trusted network. IPsec is implemented for IPv4 and provides integrity protection, data encryption, replay protection, and node authentication.



8.1.3 Benefits

It is recommended to use IPsec as a means to control access to an operator's trusted domains (core network and O&M network) and/or to create a secure VPN connection for traffic sent over an untrusted network, e.g. a leased service or public network.

8.1.4 Description

IPsec for Host provides integrity protection, data encryption, replay protection, and node authentication for IPv4 traffic. The feature consists of the following sub-features:

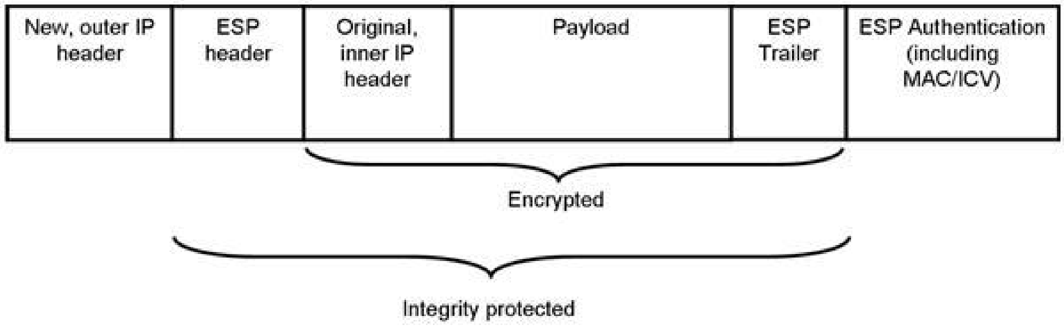
- IPsec Encapsulating Security Protocol (ESP) in Tunnel Mode;
- IKEv2 protocol for control and establishment of security associations (SAs);
- X.509 certificates with the certificate management protocol SCEP.

The mandatory IPsec security protocol Encapsulating Security Payload (ESP) is implemented. The optional protocol Authentication Header (AH) is also supported, but it is recommended to only use ESP. It is possible to configure the security associations to use NULL encryption in order to get the same behavior provided by AH when using ESP.

The following security features of ESP are supported.

- **Confidentiality -** provided through encryption of the inner IP packet when sent through the IPsec tunnel.
- **Integrity service** - provided through a Message Authentication Code (MAC), calculated and added to the inner IP packet. The MAC is verified by the IPsec function in the other end of the IPsec tunnel when a packet has been received.
- **Data origin authentication** - provided indirectly as a result of binding the key used to verify the integrity to the identity of the IPsec peer.
- **Anti-replay protection** - provided through sequence numbering of packets.

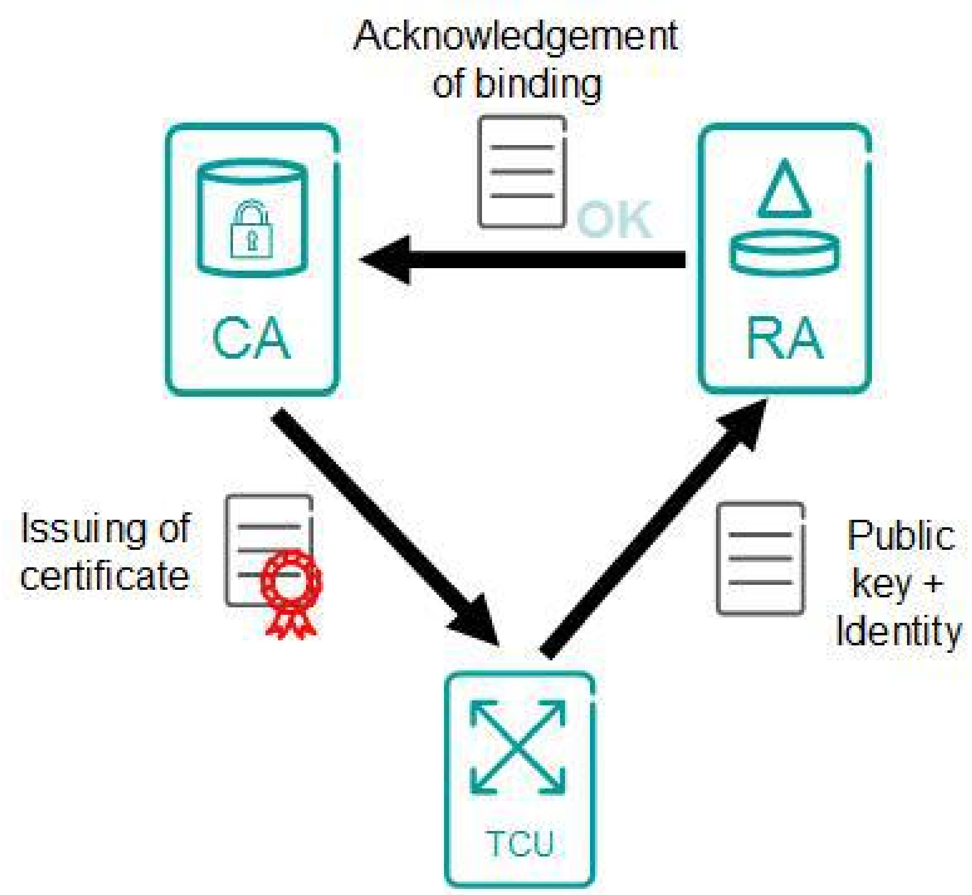
The IPsec standard specifies two modes of operation: tunnel mode and transport mode. The SIU/TCU supports tunnel mode of operation as illustrated in the diagram below. Tunnel mode implies there are different IP addresses for the tunnel end-point (the outer IP address) and for the host that provides the IP bearer service access (the inner IP address).



The *outer IP address* is the address that terminates the IPsec tunnel. This is the address in the headers of IP packets sent through the un-protected network. The outer IP address is associated to an IP interface.

The *Inner IP address* is the address in the VPN that the application uses to send and receive IP packets. Since the inner IP address is part of the encrypted inner IP packet this address is hidden in the unprotected network, the true source of the original packet is concealed. The inner IP address is the address that is visible to the BSC and the O&M network.

To handle IPsec processing for tunnels between IPsec peer nodes, IPsec automatically negotiates Security Associations (SAs) by using the second version of the Internet Key Exchange protocol (IKEv2). The authentication procedures are implemented according to IKEv2 which provides a means for mutual authentication of IPsec peers. This is performed using either X.509v3 certificate based or pre-shared keys (PSK). Digital certificates are provisioned and managed by the operator's Public Key Infrastructure (PKI). Note that configuring manual SAs is also supported for lab testing and trouble shooting.



Redundant SEG without state replication will be seen from the TCU as two IKE peers, but it is in this case useful to attempt to see one as primary and the other as standby. In order to handle automatic and transparent failover of the SEG we use two similarly policy configured IPsec tunnels, but distinguished with priorities, so only traffic is sent to the tunnel with highest priority, and if the primary SEG fails (detected by IKE DPD) then the tunnel with low priority is used instead. Note: a redundant SEG configuration with state replication is transparent to the SIU/TCU.

The OSS-RC implements a large part of the PKI, and the TCU typically connects to the RA in OSS-RC for certificate management with SCEP.

8.1.4.1 Standards

RFC 4301 Security Architecture for the Internet Protocol,RFC 4303 IP Encapsulating Security Payload (ESP),RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH),RFC 5996 Internet Key Exchange (IKEv2) Protocol,RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2),Draft-nourse-scep-23 Simple Certificate Enrollment Protocol,3GPP TS 33.210 3G security; Network Domain Security (NDS); IP network layer security,3GPP TS 33.310 Network Domain Security (NDS); Authentication Framework (AF),3GPP TS 33.401 3GPP System Architecture Evolution (SAE); Security architecture

9 TDM package - OPTIONAL FEATURES

9.1 Circuit Emulation

Feature Identity:	FAJ 121 0679/2, Rev. B
Feature Type:	Optional in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, ETSI, ANSI

9.1.1 Attention

Commercial attention

Commercial attention: Requires RFC 5086 capable Pseudowire equipment at the head end.

Dependencies

This Feature has no dependencies.

9.1.2 Summary

The Circuit Emulation (CES) feature enables the TCU/SIU to backhaul TDM based equipment over IP networks. The TDM service provided is structured E1/T1s with support for 1-31/24 DS0s per E1/T1.

The main use-case is backhaul of legacy RBSs that cannot or will not be upgraded to native IP. An example is Ericsson RBS 2000 equipped with cTRUs.

The system solution requires a pseudo-wire gateway at the head-end supporting circuit emulation according to RFC 5086.

9.1.3 Benefits

Using this feature, the customer is able to backhaul legacy RBSs and other TDM based equipment over an IP based network.

Moving from a TDM based transport network to one based on IP enables higher capacities at lower costs. To fully utilize IP networks and to avoid operating parallel transport infrastructures it is important to be able to move all traffic on an RBS site to IP.

9.1.4 Description

This feature implements a pseudo-wire for structured (N*DS0) TDM links in accordance with IETF RFC 5086 (CESoPSN) and ITU-T Y1453. The feature implements the following common subset of these standards:

- Support for structured TDM only. 1-24 DS0s per T1 pseudo-wire or 1-31 DS0s per E1 pseudo-wire
- Only UDP/IP encapsulation is supported. RTP is not used.

The SIU can support up to 16 pseudo-wires simultaneously (TCU can support 8). Each E1/T1 port on the TCU/SIU can be mapped to only one pseudo-wire. Unused DS0s on that port **cannot** be used for other purposes i.e for another pseudo-wire or for Abis lower towards an RBS.

The different pseudo-wires are individually configured with respect to packetization latency and jitter buffer size. Each pseudo-wire can terminate in a different pseudo-wire gateway.

9.1.4.1 Standards

RFC 5086

9.1.5 Enhancement

N/A

9.2 IP over E1/T1

Feature Identity:	FAJ 121 0677/3, Rev. B
Feature Type:	Optional in T11B, T12A, T12B, T13B, T14A, T14B
Technology:	GSM, WCDMA, ETSI, ANSI, GRAN

9.2.1 Attention

Commercial attention

Not applicable

Dependencies

No internal technical dependencies have been defined for this Feature

9.2.2 Summary

With IP over E1/T1, the benefits of IP transport can be realized on sites with TDM-based WAN transmission. Functions like Multi TG, Site LAN, Abis Local Connectivity and Transport sharing are also available over an E1/T1 backhaul network. Multiple ML-PPP instances can be configured so it is possible to use ML-PPP bundles in both CDMA RBS connections and WAN links.

9.2.3 Benefits

All current and future functionality of the Abis over IP feature can also be used over an E1/T1 backhaul network. Specifically;

- Multi TG gives additional bandwidth savings for larger sites. This depends on traffic load and RBS configuration, but typically sites with more than 10 TRXs will benefit.
- Increased reliability as, for instance, the loss of one E1 (if more than one E1 is used for the site) will not directly affect individual TRXs.
- Abis Local Connectivity can be used with E1/T1 backhaul
- Transport sharing reduces backhaul costs when WCDMA is introduced to an existing GSM network

- The Site LAN feature makes it possible to attach modern LAN based site equipment without the need for extra Bridges or Routers to handle E1/T1 backhaul

Finally, any operator with a clear migration strategy to IP can deploy an all IP network over their existing PDH/SDH infrastructure.

Operator Value

The commercial value of using IP over E1/T1 falls into different categories.

- Operators with a clear migration strategy towards an All-IP network. Here the IP over E1/T1 means that a true All-IP backhaul can be launched cost-effectively where only leased E1/T1 capacity is available. The value comes from a strategic perspective in combination with the operational efficiency of running only one network technology in RAN.

- With the SIU/TCU the traffic from the whole base station site is aggregated (Multi-TG) and optimized (with Abis optimization). For larger sites or sites with many transceiver groups (specifically with uneven TRX distribution between the transceiver groups) this improves efficiency above the Abis Optimization feature.

- Operators wanting to introduce WCDMA while minimizing the increase in backhaul costs. Together with the Transport Sharing feature this will enable an operator to introduce WCDMA by adding only one E1/T1 and pooling bandwidth between GSM and WCDMA. During off-peak hours the full backhaul bandwidth can then be used for services such as HSPA.

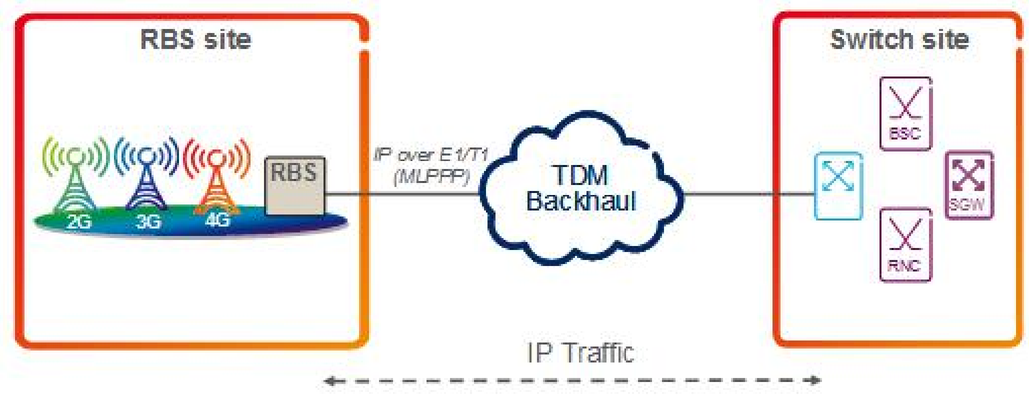
- CDMA operators can connect RBSs to the SIU/TCU via ML-PPP bundled links, and then (if required) use another bundled link for the WAN connection. Traffic forwarding from ML-PPP to IP/Ethernet WAN is also supported.

9.2.4 Description

The feature requires the SIU/TCU at the RBS site to provide IP over E1/T1 connections using ML-PPP. The SIU provides sixteen E1/T1 ports, the TCU has eight; these are shared completely flexibly between GSM/CDMA RBS connections and the IP over E1/T1 WAN. The E1/T1s may be bundled using ML-PPP, and multiple ML-PPP instances can be configured. The maximum bundle size is eight links, and a maximum of four bundles (i.e. four ML-PPP instances) can be configured within the 16 or 8 E1/T1 ports.

In a typical implementation the WAN connection will use two, four or eight E1/T1 links in a single ML-PPP bundle; connections to CDMA RBSs consist of typically two or four bundled E1/T1s.

A router at the switching site terminates the ML-PPP bundles and routes the IP packets to the BSC/RNC. The feature has been verified using SmartEdge and Tellabs equipment within the IP RAN solution, and interoperability has also been demonstrated with other third-party switching site equipment. The figure below gives an overview of the feature.



The SIU/TCU and the ML-PPP router will provide link layer support for transporting IP packets over E1/T1 circuits based on the Point-to-Point Protocol (PPP) and Link Control Protocol (LCP) according to RFC1661, RFC1662, RFC1570, RFC 1990 and RFC2686.

Error detection is performed on individual links. If a link failure is detected automatic reestablishment is started.

Synchronization of SIU/TCU/RBS can be achieved using the clock information from the E1/T1s or by using NTP packets from a timeserver.

9.2.4.1 Standards

RFC1661, RFC1662, RFC1570, RFC 1990, RFC2686.

9.2.5 Enhancement

Nothing specific